




# 攻防世界 Crypto高手进阶区 2分题 工业协议分析2

原创

思源湖的鱼  于 2020-12-03 13:45:08 发布  136  收藏

分类专栏: [ctf](#) 文章标签: [ctf](#) [攻防世界](#) [crypto](#) [流量包](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_44604541/article/details/110528921](https://blog.csdn.net/weixin_44604541/article/details/110528921)

版权

## CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

### 前言

继续ctf的旅程

攻防世界Crypto高手进阶区的2分题

本篇是工业协议分析2的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

### 解题过程

得到一个流量包

有大量的UDP包

733	100.430392	192.168.1.181	192.168.1.123	UDP	173	11000 → 64406	Len=131
648	91.813108	192.168.1.123	192.168.1.181	UDP	179	64406 → 11000	Len=137
9	0.329000	192.168.1.243	239.255.255.250	SSDP	216	M-SEARCH	* HTTP/1.1
26	1.330596	192.168.1.243	239.255.255.250	SSDP	216	M-SEARCH	* HTTP/1.1

> Frame 733: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface \Device\NPF\_{A1A8295F-...}

> Ethernet II, Src: 00:e2:36:0b:19:2b (00:e2:36:0b:19:2b), Dst: VMware\_0a:63:9f (00:0c:29:0a:63:9f)

> Internet Protocol Version 4, Src: 192.168.1.181, Dst: 192.168.1.123

> User Datagram Protocol, Src Port: 11000, Dst Port: 64406

Source Port: 11000

Destination Port: 64406

Length: 139

Checksum: 0x3122 [unverified]

[Checksum Status: Unverified]

[Stream index: 4]

> [Timestamps]

0000	00 0c 29 0a 63 9f 00 e2 36 0b 19 2b 08 00 45 00	..).c... 6...+..E.
0010	00 9f 6b 5b 00 00 80 11 4a 72 c0 a8 01 b5 c0 a8	..k[.... ]r.....
0020	01 7b 2a f8 fb 96 00 8b 31 22 4c 00 4f a1 83 00	..{*..... 1"[-0...
0030	e3 00 25 27 25 27 11 00 62 00 00 00 00 00 00 00	..%'%'.. b.....
0040	00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 18	.....
0050	00 00 00 38 00 00 00 2a 00 00 00 62 00 00 00 00	...8...* ...b....
0060	00 00 00 62 00 00 00 00 00 00 00 00 02 14 00 4d	...b.... .....M
0070	41 49 4e 5f 28 d6 f7 b3 cc d0 f2 29 00 03 01 02	AIN_(... ..)....
0080	00 c8 00 00 01 00 25 00 36 36 36 63 36 31 36 37	.....%· 666c6167
0090	37 62 33 37 34 36 36 66 34 64 33 32 35 33 37 34	7b37466f 4d325374
00a0	36 62 36 38 36 35 35 30 37 61 37 64 00	6b686550 7a7d·

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

找到异常包

提取字符

666c61677b37466f4d3253746b6865507a7d

瞅着是16进制

1	666c61677b37466f4d3253746b6865507a7d
2	

16进制转字符    字符转16进制    测试用例    清空结果    复制结果

**PayPal**

一个账户，收款全球。0费用开户，享卖家保障，赢逾2亿用户。

1 flag(7FoM2StkhePz) [https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

得到flag

## 结语

简单题